UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/596,009	06/16/2000	Brig Barnum Elliott	00-4010	2514

28120 7590 05/11/2006

FISH & NEAVE IP GROUP
ROPES & GRAY LLP
ONE INTERNATIONAL PLACE
BOSTON, MA 02110-2624

EXAMINER	
MOORTHY, ARAVIND K	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 05/11/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/596,009	ELLIOTT, BRIG BARNUM	
	Examiner	Art Unit	
	Aravind K. Moorthy	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 February 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-26 and 32* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-26 and 32* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *16 June 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This is in response to the arguments filed on 21 February 2006.

2. Claims 1-26 and 32 are pending in the application.

3. Claims 1-26 and 32 have been rejected.

4. Claims 27-31 and 33-36 have been cancelled.

Response to Arguments

5. Applicant's arguments filed 21 February 2006 have been fully considered but they are not persuasive.

On page 11, the applicant argues that Conklin does not teach a router that evaluates an excising signal which "indicates that a network control computer has determined that an untrusted party has gained control of a first functioning router of the plurality of routers and is to be excised from the network," as recited in claim 1.

The examiner respectfully disagrees. Conklin teaches that if there has been an intrusion, there is a signal (i.e. Trap PDU signal) to remove the device. The Trap PDU signal is used to signal the type of event. Therefore, once the signal is sent, it is known that the device (i.e. router) needs to be removed, as shown in figure 3.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. Claims 1, 2, 6-8, 10-12, 15, 16, 24-26 and 32 are rejected under 35 U.S.C. 102(e) as being anticipated by Conklin et al U.S. Patent No. 5,991,881.

As to claims 1, 7 and 24, Conklin et al discloses a communications router for use in a communications network including a plurality of routers controlled by one or more trusted parties, and at least one network control computer communicating with the communications router, the communications router comprising:

a transceiver to transmit and receive messages [column 2, lines 43-58];

an electronic memory circuit having network information stored therein [column 2, lines 43-58];

an electronic processor circuit which (i) evaluates an excising signal received from the network control computer, the excising signal indicating that the network control computer has determined that an untrusted party has gained control of a first functioning router of the plurality of routers and is to be excised from the network [column 5 line 46 to column 6 line 18]; (ii) determines an authenticity of the excising signal [column 5 line 46 to column 6 line 18]; (iii) excises the first router when the excising signal is authenticated [column 5 line 46 to column 6 line 18]; (iv) reroutes the excising signal to at least a second router of the plurality of routers when the excising signal is authenticated [column 5 line 46 to column 6 line 18].

As to claims 2 and 8, Conklin et al discloses that the electronic processor circuit excises the first router by adding the first router to information regarding routers stored in the electronic memory circuit [column 15, lines 13-42]. Conklin et al discloses removing from the electronic

memory circuit routing updates corresponding to the first router [column 15 line 52 to column 16 line 7]. Conklin et al discloses removing the first router from a neighbor table stored in the electronic memory circuit when the first router is listed therein [column 15 line 52 to column 16 line 7]. Conklin et al discloses recomputing a forwarding table to direct future routing [column 15 line 52 to column 16 line 7].

As to claim 6, Conklin et al discloses that the electronic processor reinstates the first router when the communications router receives and verifies a reinstate message from the network control computer [column 5 line 46 to column 6 line 18].

As to claims 10 and 11, Conklin et al discloses evaluating a signal received through the transceiver from another network router [column 5 line 46 to column 6 line 18]. Conklin et al discloses identifying which network router a signal has just been received from [column 5 line 46 to column 6 line 18]. Conklin et al discloses determining if the network router is identified by the information regarding excised routers [column 5 line 46 to column 6 line 18]. Conklin et al discloses discarding the signal when the router is listed [column 2, lines 51-58]. Conklin et al discloses processing the signal when the router is not listed [column 2, lines 51-58]. Conklin et al discloses processing the signal when the router is listed [column 2, lines 51-58]. Conklin et al discloses recomputing the forwarding table, as discussed above.

As to claim 12, Conklin et al discloses removing the second router from information stored in memory regarding routers controlled by trusted parties [column 5 line 46 to column 6 line 18]. Conklin et al discloses removing from the communications router routing updates corresponding to the second router [column 5 line 46 to column 6 line 18]. Conklin et al discloses removing the second router from a neighbor table of the communications router when

the second router is listed therein [column 5 line 46 to column 6 line 18]. Conklin et al discloses recomputing a forwarding table [column 5 line 46 to column 6 line 18].

As to claim 15, Conklin et al discloses the step of reinstating the second station when the communications router receives and verifies a reinstate message from the network control computer [column 2, lines 51-58].

As to claim 16, Conklin et al discloses a mobile communications station which communicates among a plurality of mobile stations controlled by a first of parties in an ad-hoc network in which stations are arranged in clusters of communication member stations, with one member station in each cluster being a head station for the cluster, each member station communicating with the network through at least on cluster head station, a cluster head station communicating with zero or more cluster head stations, a network linked with the mobile communications station, the mobile communications station comprising:

a transceiver which transmits signals to and receives signals from other mobile stations in the network,

a memory having network information stored thereon [column 5 line 46 to column 6 line 18];

a processor which (i) operates the mobile station as a cluster head or cluster member station [column 5 line 46 to column 6 line 18]; (ii) evaluates an excising signal received from the network control computer, the excising signal indicating that the network control computer has determined that an untrusted party has gained control of a first functioning cluster head or cluster member station and is to be excised from the network; (iii) verifies the authenticity of the

excising signal; (iv) excises the first cluster head or cluster member station when the excising signal is authentic; and (v) distributes the excising signal to at least a second cluster head or cluster member station [column 5 line 46 to column 6 line 18].

As to claims 25 and 26, Conklin et al discloses in a communications system for communications among a plurality of routers in a network controlled by one or more trusted parties, at least on computer being linked to a first router of the plurality of routers, a method of operating the network comprising the steps of:

authenticating in the first router a cut-off signal received from the control computer, the cut-off signal indicating that the control computer has determined that at least on functioning router is controlled by an untrusted party and is to cut-off from communicating with the network [column 5 line 46 to column 6 line 18];

preventing the first router from communicating with the at least one cut-off router when the signal is authenticated [column 5 line 46 to column 6 line 18];

redistributing the cut-off signal to each of the plurality of routers, except for the at least one cut-off router, and preventing each of the remaining routers from communicating with the at least one cut-off router [column 5 line 46 to column 6 line 18],

wherein when a router receives a message from one of the plurality of routers, the router determines if the message is from the at least one cut-off router,

and processes the message only when the message is not from the at least one cut-off router [column 5 line 46 to column 6 line 18].

As to claim 32, Conklin et al discloses computer executable code stored on a computer readable medium, the code to operate a communications router in a network having a plurality of routers controlled by one or more trusted parties, at least one computer being linked to the communications router, each of the plurality of routers including a transceiver to transmit and receive messages, the computer executable code comprising:

code to excise from the network a functioning router that has become controlled by an untrusted party , as discussed above;

code to verify that messages transmitted among the plurality of routers are from routers controlled by trusted parties, as discussed above;

code to reinstate an excised router when a trusted party regains control of the excised router, as discussed above.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 3, 4, 9 and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Conklin et al U.S. Patent No. 5,991,881 as applied to claim 1 above, and further in view of Raz et al U.S. Patent No. 6,529,515 B1.

As to claims 3, 9 and 13, Conklin et al does not teach that the electronic processor circuit further causes a message to be transmitted to the network control computer and to disregard the excising signal when the excising signal is not authentic.

Raz et al teaches a message to be transmitted to the network control computer and to disregard the excising signal when the excising signal is not authentic [column 8, lines 9-27].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Conklin et al so that a message would have been transmitted to the network control computer and to disregard the excising signal when the excising signal is not authentic.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Conklin et al by the teaching of Raz et al because it provides efficient use of network resources, without increasing the complexity of application development. Advantageously, it enables the safe execution and rapid deployment of new distributed management applications in a network layer. This active network approach can be gradually integrated into, e.g., an otherwise conventional IP network, and allows smooth migration from conventional IP to programmable networks [column 3, lines 5-15].

As to claim 4, Conklin et al as modified teaches that the electronic processor circuit further evaluates a signal received through the transceiver from another network router. Conklin et al as modified teaches identifying which network router the signal has been received from

[column 7, lines 16-60]. Conklin et al as modified teaches determining if the network router is listed with the information regarding excised routers. Conklin et al as modified teaches discarding the signal when the router is listed. Conklin et al as modified teaches processing the signal when the router is not listed [column 7, lines 16-60].

8. Claims 5 and 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Conklin et al U.S. Patent No. 5,991,881 as applied to claim 1 above, and further in view of Applied Cryptography (hereinafter Schneier).

As to claims 5 and 14, Conklin et al does not teach that the electronic processor circuit determines the authenticity of the excising signal using a public encryption key.

Schneier teaches the use and benefits of public key encryption [pages 461-462].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Conklin et al so that the electronic processor circuit would have determined the authenticity of the excising signal using a public encryption key.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Conklin et al by the teaching of Raz et al because public-key is designed to resist chosen-plaintext attacks, their security is based both on the difficulty of deducing the secret key from the public key and the difficulty of deducing the plaintext from the cipher text [page 462].

9. Claims 17-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Conklin et al U.S. Patent No. 5,991,881 in view of Chaum U.S. Patent No. 4,947,430.

As to claims 17, 19 and 22, Conklin et al discloses formulating in the control computer an excise signal indicating that an untrusted party has gained control of at least a second functioning router to be excised from the network [column 13, lines 47-63]. Conklin et al discloses adding the information identifying the second router to information regarding excised routers stored in memory of the first router [column 14 line 61 to column 15 line 51]. Conklin et al discloses removing from the first router routing updates corresponding to the second router [column 14 line 61 to column 15 line 51]. Conklin et al discloses removing information corresponding to the second router from a neighbor table of the first router when the second router is listed therein [column 15 line 51 to column 16 line 7]. Conklin et al discloses recomputing a forwarding table in the first router. Conklin et al discloses redistributing the excise signal to each of the plurality of routers, except for the second router [column 15 line 51 to column 16 line 7]. Conklin et al discloses upon receiving a message from another one of the plurality of routers, determining, in each of the plurality of routers an identifier for the router from which the message is received and processing the message only when the information regarding excised routers does not include the identifier authentic [column 16, lines 41-63].

Conklin et al does not teach providing a digital signature of the control computer on the excise signal and transmitting the excise signal to the first router. Conklin et al does not teach verifying the signature on the excise signal in the first router. Conklin et al does not teach that the digital signature is validated using a public encryption key.

Chaum teaches providing a digital signature of the control computer on the excise signal and transmitting the excise signal to the first router. Chaum teaches verifying the signature on the excise signal in the first router [column 3, lines 29-42]. Chaum teaches that the digital signature is validated using a public encryption key [column 8, lines 27-46].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Conklin et al so that a digital signature would have been provided for the control computer. The digital signature would have been verified on the excise signal in the first router. The digital signature would have been validated using a public key.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Conklin et al by the teaching of Chaum because it requires consent every time the signature is verified and provides a binding signature that cannot be forged to authenticate a user [column 2, lines 36-46].

As to claims 18 and 23, Conklin et al teaches the steps of transmitting a message to the control computer from the first router and causing the first router to disregard the excise signal each when the excise signal is not authentic, as discussed above.

As to claim 20, Conklin et al teaches the step of reinstating the excised second router, as discussed above.

As to claim 21, Conklin et al teaches that a router disregards the message when the information regarding excised routers includes the identifier, as discussed above.

Conclusion

10. THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K. Moorthy whose telephone number is 571-272-3793. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Aravind K Moorthy
May 6, 2006

CHRISTOPHER REVAK
PRIMARY EXAMINER
5/9/06